viadex® Global IT Service Partner
FULCRUM IT PARTNERS

Powered by iland®

Three Threats to Your Office 365 Data: One Solution

Using Office 365 Backup to Save Your Data From Ransomware, Insider Threats and Accidents

You probably can't exaggerate how much your organization relies on email. From valuable contacts to the vital messages themselves to the often sensitive attachments, email systems contain some of the most important data in any organization. Your office productivity suite and the documents, notes and spreadsheets your employees create with it are equally vital. Unfortunately, in both cases protecting that data is increasingly challenging. External threats like ransomware are ever-present, while malicious insiders and plain old accidents can be difficult to stop and equally—if not more—damaging.

Fortunately, there is a single solution that can prevent, or mitigate, all three of these common threats. By adding cloud-based backup to your Office 365 instance, you can protect valuable emails, contacts, and files in Exchange Online, SharePoint Online and OneDrive from the worst results of ransomware, insider attacks and accidents.

Holding Productivity Ransom

Today, your email, documents and apps are under constant attack from external threats. Many security experts now say that it is not a question of whether you will be attacked, but when. And nothing seems to strike more fear in business users today than ransomware.

> "...it is not a question of whether you will be attacked, but when."

Ransomware is a malicious program that infects a device and either encrypts or blocks access to data until the victim pays a ransom. It has existed for many years, but has recently exploded in popularity, becoming the most common variety of malicious code.[1] Once it strikes, it is difficult to defeat without paying, and because perpetrators request payment through anonymous tools such as cryptocurrency, they are rarely caught.

Imagine urgent emails, office documents and spreadsheets, and years' worth of contacts suddenly being kept from you and the users you support. Not only can you no longer get to your email or files, you likely cannot use your device at all. The criminals have completely robbed everyone in your business of the ability to work. The thought should be enough to skyrocket the stress of any IT professional, and in the spring of 2017, it happened to thousands of them.

A Victory, but Not for the Encrypted Data

The first instances of the ransomware variant WannaCry appeared in the spring of 2017. By May 12, security company Avast had detected 250,000 instances of WannaCry[2] but others believe that totals eventually exceeded 400,000.[3]

The attack shut down hospitals, banks and businesses of all kinds. Staff could not get to emails, applications or documents. Valuable data, contacts and files were suddenly locked down. The very lifeblood of many of these organizations was trapped behind ransom notes.

Few cybersecurity stories end happily. But shortly after WannaCry roared into action, a security researcher noticed that by purchasing a specific domain referenced in the ransomware code, the researcher could stop the software. In moments, the WannaCry plague was halted.

But this remarkable victory for security researchers didn't help those already infected. Hundreds of thousands of computers remained encrypted. How many were prepared with full backups of their data?

Preventing external attacks is a topic worthy of an entire library of papers. Office 365 itself provides some tools to help. Unfortunately, as many security researchers admit, preventing every attack is likely impossible. While 29 percent of organizations expect to cope with ransomware by having network security or endpoint security programs catch the attack, only 13 percent of organizations that actually saw ransomware attacks were saved by their security programs.[4] You have to be prepared for the aftermath.

For many, the aftermath of a ransomware attack often involves starting over. 451 Research found that when struck with ransomware, 82 percent of organizations simply reimaged the infected computer. Some of those organizations were luckier than others, however. Sixty-eight percent of attacked organizations could reimage and restore from a backup, but 14 percent had to start over without any of their original data.[5]

The Threat Within

Despite the growth of ransomware and the other cyber threats that make the news, the second most prevalent cause of cyber security issues, according to the Verizon Data Breach Investigations Report, is privileged misuse.[6] This covers any unapproved or malicious use of organizational resources.

> "Gartner saw a 50 percent year-over-year increase in customers asking about security against insider threats."

According to a blog written in the spring of 2018 by analyst Avivah Litan, Gartner saw a 50 percent year-over-year increase in customers asking about security against insider threats.[7] And while solutions do exist, none are foolproof. That's because insiders already have access to much of the valuable data organizations need to protect and often have legitimate business reasons to access and transmit that data.

How can organizations possibly prepare for such threats? As with external threats, the key is to limit the possible damage and discover misdeeds quickly. We'll look at how to do that after we examine one more persistent threat.

"Oops": The CIO's Least Favorite Word

It would be nice to believe that malware and angry former employees were the IT department's only challenges, but unfortunately, the average accident can do just as much damage. Every day, employees delete important emails, files and entire folders, corrupt files, send documents to the wrong recipients and otherwise "oops" their way into IT's angry crosshairs. In fact, accidents are the second most prevalent cause of data breaches after web app attacks, according to the Verizon Data Breach Investigations Report.[8]

> "Accidents are the second most prevalent cause of data breaches after web app attacks,..."

Good employee training and internal processes can help prevent some accidents, but human nature being what it is, will never eliminate them all. Cloud email and productivity solutions, such as Office 365, also provide enormous help by backing up inbox and folder data, deleted items and more.

However, Microsoft does not store Office 365 data forever, meaning that if employees do not notice the accident immediately, there may be no chance to recover that data. That doesn't have to be the case, however, if your organization invests in backing up Office 365 with a cloud-based backup solution.

Modern Productivity Protection

As we've seen, a cloud email and office productivity program, like Office 365, can help tackle many of the challenges above. Office 365 offers security features like encryption, which can help prevent certain external attacks from snooping on your messages, and options to protect against unsafe attachments and links.

> "What if the data at risk in ransomware attacks, insider misuse and accidents wasn't at risk after all?"

Ultimately, though, Office 365 cannot prevent all attacks. Insiders can sidestep many of these protections and if employees are allowed to use personal email on work devices, they can infect their machines that way. But what if the data at risk in ransomware attacks, insider misuse and accidents wasn't at risk after all? Suddenly, these vexing problems become far more manageable.

Cloud-based backup offers many advantages over on-premises systems, such as the ability to leverage the scalability and flexibility of the cloud while escaping the burden of building and managing additional infrastructure. Backup solutions can recover a system either in a short period of time, or in some cases, instantaneously.

But isn't a cloud product like Office 365 already providing backups? After all, Microsoft runs Office 365 in its secure data centers, so you always have access to it. Don't you? The answer to that question is yes, but often not to the extent organizations think, and need, for true protection from cyber threats.

Whereas a backup solution, such as from software vendor Veeam, can back up all your data, Office 365 only backs up some of your data, and only for a certain period of time. In most cases, Office 365 backups are only held by Microsoft for 30 days while Veeam offers much more flexibility, including unlimited file retention.

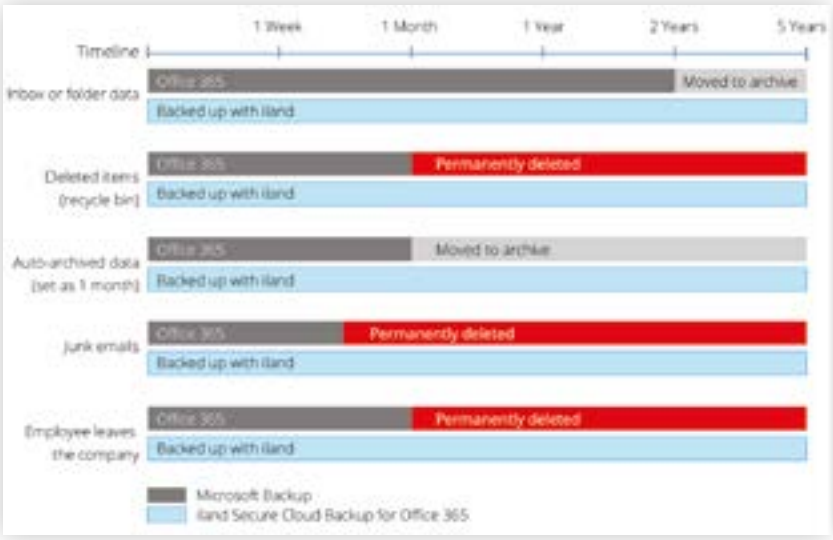
One particularly relevant example is when an employee leaves a company. Microsoft saves that employee's data for 30 days, after which it is permanently deleted. If your organization realizes too late that it needs the information contained in that former employee's email or files, you will be out of luck.

Microsoft Office 365 also discards recycle bin items after 30 days. While this may seem sufficient, consider the case of a malicious insider or disgruntled employee deleting valuable documents. It often takes months for organizations to discover cyber security incidents. Without a secure cloud backup, that valuable information will be gone long before your organization realizes what the employee has done.

Thus, for true peace of mind, organizations should combine Office 365 with a cloud-based backup solution.

Cloud-Based Backup for Office 365

Cloud-based backup as an ideal solution to many of the threats facing organizations' productivity today. In an article on protecting organizations from cyber and ransomware attacks, Gartner suggests



This chart shows the amount of time Office 365 saves data versus the unlimited retention and storage available with iland Secure Cloud Backup for Office 365.

you "backup copies of your files and have them stored elsewhere. Cloud-based services are often unaffected by such incidents, but local and network copies of files are likely to be at risk."[9]

Because a malicious insider would have to have access to your cloud backup—a highly unlikely scenario—to completely erase data, a cloud-based backup solution provides enormous protection from insiders. You can rest easy knowing you always have a trusted saved copy of your data available. This is equally helpful in the case of many of the most common accidents. If an employee deletes or mistakenly corrupts a valuable file, a trusted copy awaits in your backup solution.

> "iland Secure Cloud Backup for Office 365 offers unlimited storage and retention, so you can keep as much as you want for as long as you want."

Backup solutions are designed so that if a threat makes its way through your other defenses, you can minimize the damage done and bounce back quickly. And the key to knowing you can bounce back quickly is finding the right backup partner.

iland Secure Cloud Backup for Office 365

One example of a backup solution tailored to help support your Office 365 installation is iland's Secure Cloud Backup offering powered by Veeam. The solution offers a cloud repository that automatically backs up Office 365 users' data (including mail, calendar, contacts, SharePoint, and OneDrive).

The solution backs up data daily and provides unlimited storage and unlimited retention, so you can keep as much as you want for as long as you want. This unlimited retention can be vital for security and compliance purposes, allowing you to keep up with more stringent policies and regulations.

iland Secure Cloud Backup for Office 365 offers multiple recovery options in the event that something does go wrong. You can:

- Restore mailbox, SharePoint, and OneDrive data directly into Office 365.
- Export objects to a Personable Storage Table (.pst) file.
- Save Exchange items as a Microsoft Exchange Mail Document (.msg) file.
- Send items as attachments to specified recipients.
- Directly download individual objects as files or groups of objects as a .zip file.

By combining the power of Veeam's backup tools with iland's Secure Cloud, iland Secure Cloud Backup for Office 365 can help shelter you against external threats and keep data protected from deletion and loss.

Backup Providing Peace of Mind

Sophisticated and powerful security tools exist for IT, but none have succeeded in eliminating the threat to your data and applications. But this truth does not mean you need to despair. iland's Office 365 backup offering provides a way to survive external attacks, insider misuse and the clumsiest of clicks. By pairing Office 365 with a reliable cloud-based backup, your organization can move past ransomware, angry former employees and accidents faster to stay focused on your business and your growth.

Next Steps

Ready to fully protect your Office 365 data? Learn more about iland Secure Cloud Backup℠ for Microsoft Office 365 with Veeam.

---

[1] Verizon Data Breach Investigations Report, 2018.
[2] The Five Biggest Ransomware Attacks of the Last 5 Years, Josh Fruhlinger, CSO Online, Aug 2017 https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-the-last-5-years.html
[3] WannaCry Ransomware Statistics: The Numbers Behind the Outbreak, Jonathan Crowe, Barkley, May 2017. https://blog.barkly.com/wannacry-ransomware-statistics-2017
[4] Voice of the Enterprise: Information Security, Workloads and Key Projects 2018, 451 Research
[5] Ibid.
[6] Verizon Data Breach Investigations Report, 2018
[7] Emerging Insider Threat Detection Solutions, Avivah Litan, Gartner, April 2018. https://blogs.gartner.com/avivah-litan/2018/04/05/insider-threat-detection-replaces-dying-dlp/
[8] Verizon Data Breach Investigations Report, 2018.
[9] Protect Your Organization From Cyber and Ransomware Attacks, Laurence Goasduff, Gartner, Feb 2018. https://www.gartner.com/smarterwithgartner/protect-your-organization-from-cyber-and-ransomware-attacks/

viadex® Global IT Service Partner
FULCRUM IT PARTNERS

Email: services@viadex.com

Web: www.viadex.com

Europe:
+44 208 739 1000

Africa:
+27 21 001 1175

Asia:
+65 31388160

Americas:
+1 833 847 3845

United Arab Emirates:
+971 4 512 4156

Viadex Ltd, Unit 20, Red Lion Business Park, Red Lion Road, Surbiton, KT6 7QD, UK